



Date de réception : 23/01/2015

WRITTEN OBSERVATIONS OF THE REPUBLIC OF POLAND

Case C-362/14*

Document lodged by:

Republic of Poland

Usual name of the case:

Schrems

Date lodged:

6 November 2014

* Language of the case: English.

Warsaw, 6 November 2014

**TO THE PRESIDENT AND MEMBERS OF THE COURT OF JUSTICE
OF THE EUROPEAN UNION**

WRITTEN OBSERVATIONS

OF THE REPUBLIC OF POLAND

submitted pursuant to Article 23 of the Statute of the Court of Justice in the
proceedings for a preliminary ruling in Case

C-362/14 *Schrems*

(national court: High Court of Ireland — Ireland)

Agent of the Republic of Poland:

Bogusław Majczyna

Address for service:

Ministerstwo Spraw Zagranicznych

al. J. Ch. Szucha 23

00-580 Warsaw — POLAND

Table of contents

I. — Facts of the case and questions referred	I – 4
II. Position of the Republic of Poland.....	I – 5
II.1. Obligation to apply Decision 2000/520 in the context of irregularities in the implementation of the Safe Harbour scheme	I – 5
II.2. Possibility of authorities of a Member State suspending the transfer of data to the United States.....	I – 7
II.3. Transfer of personal data to the United States in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.....	I – 8
III. Proposed decision	I – 11

I. — Facts of the case and questions referred

- 1 The request for a preliminary ruling in Case C-362/14 *Schrems* has been made by an Irish court (High Court of Ireland). It concerns proceedings before that court relating to the transfer of personal data to the United States of America under Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.¹
- 2 As is clear from the grounds of the request, the dispute has arisen against the background of the following facts. Proceedings brought by an Austrian national are under way before the Irish court. In those proceedings that person challenges a decision of the Irish Data Protection Commissioner not to investigate his complaint concerning the transfer to the United States of his personal data processed in the Facebook social network.
- 3 The personal data of European users of that network are transferred to servers located within the United States and are processed there. Both Facebook Inc., a company incorporated under Californian law, and Facebook Ireland self-certify pursuant to the Commission's Safe Harbour decision. However, in the proceedings the applicant argues that the revelations made in 2013 by Edward Snowden concerning the activities of the US National Security Agency under the PRISM programme show that there is no meaningful protection in respect of data transferred from the European Union to the United States under the Safe Harbour regime.
- 4 Against that background, the Irish court (High Court of Ireland) decided to refer the following questions to the Court of Justice:

Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC) having regard to Article 7, Article 8 and Article 47 of the Charter of Fundamental Rights of the European Union, the provisions of Article 25(6) of Directive 95/46/EC notwithstanding?

Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published?

¹ OJ 2000 L 215, p. 7.

II. Position of the Republic of Poland

II.1. Obligation to apply Decision 2000/520 in the context of irregularities in the implementation of the Safe Harbour scheme

- 5 The EU system for protection of personal data arising from Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data² is based on a general prohibition on the transfer of personal data to third countries unless those countries ensure an adequate level of protection of those data. In light of the fundamental differences in the European and US systems for the protection of personal data, the United States must in principle be regarded as a country which does not, in terms of the protection of personal data, meet standards which ensure an adequate level of protection. Therefore, in accordance with the principles laid down in Directive 95/46, data can flow from the European Union to the United States only under particular conditions. One of the bases for transferring personal data to the United States is Decision 2000/520, which lays down the conditions governing the transfer of personal data for commercial purposes. That decision permits the free transfer of personal data from the Member States of the European Union to organisations in the United States, which voluntarily undertake to abide by the principles laid down in the decision.³
- 6 More than a decade has passed since the adoption of Decision 2000/520. However, not only the passage of time and the constant development of the information society, which has substantially changed the reality of trade, are relevant to the present case. The perception of Decision 2000/520 has also been affected significantly by the revelation in 2013 of details of the activities of the US National Security Agency under the PRISM programme. It is clear from the information that has been revealed that certain US organisations certified under the Safe Harbour regime make personal data that they hold available to US intelligence services, including the National Security Agency, which are deliberately and systematically conducting large-scale data collection programmes. The practical implementation of the Safe Harbour principles by the

² OJ 1995 L 281, p. 31.

³ Highlighting the importance of this case, it should be noted that that decision forms the basis for an increasingly broad exchange of personal data. According to the information provided by the European Commission in the Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows (COM (2013) 846 final), around 400 bodies belonged to the Safe Harbour scheme in 2004, but in 2013 the number was over 3 200. The major players in the Internet and new technologies sector belong to the scheme.

US side, which failed to meet the European Union's expectations for many years, is also relevant in this regard.⁴

- 7 The discrepancy between the findings on which Decision 2000/520 was based and the actual level of protection for personal data in the United States is therefore marked. It is identified *inter alia* by the referring court, which held that, although the surveillance and interception of personal data transferred from the European Union to the United States by the National Security Authority serve legitimate and necessary counter-terrorism objectives and goals, it is clear from the information revealed that the US authorities significantly exceeded their powers and EU citizens whose data were processed did not have adequate entitlement as regards protection of their rights. The referring court held that the information revealed by Edward Snowden is accurate and found that personal data transferred by Facebook Ireland to its parent company in the United States is capable of being accessed by the National Security Authority and other US federal agencies in the course of a mass and indiscriminate surveillance and interception of such data.
- 8 The risk is also identified by the European Commission itself which has acknowledged that '[l]arge-scale US intelligence collection programmes, such as PRISM affect the fundamental rights of Europeans and, specifically, their right to privacy and to the protection of personal data'.⁵ With regard to Decision 2000/520 the Commission has acknowledged that, '[g]iven the weaknesses identified, the current implementation of Safe Harbour cannot be maintained'.⁶
- 9 Despite the seriousness of the weaknesses identified, the Commission decided not to revoke Decision 2000/520 on account of the anticipated adverse effect of such a move on the interests of companies in the European Union and the United States. Instead the Commission foresaw the need for thorough strengthening of that decision.⁷ The Republic of Poland considers that the fact itself that there are weaknesses in the implementation of Decision 2000/520 has no bearing on the lawfulness thereof and on the fact that the Member States are bound by it. Since Decision 2000/520 has not been revoked in spite of reports of its weaknesses, the Member States, and thus their national authorities for the protection of personal data, are required to apply it. According to the case-law of the Court of Justice, decisions, like other acts of EU law, are presumed to have a lawfulness which

⁴ Concerns about the enforcement of the Safe Harbour scheme are expressed directly, *inter alia*, by the European Commission; see in particular paragraphs 2.2, 3, 4, 5 and 5.1 of the Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847.

⁵ COM(2013) 846 final, p. 3.

⁶ COM(2013) 846 final, p. [7].

⁷ See Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final.

cannot be revoked other than by a judgment of the Court of Justice.⁸ The obligation on a Member State to apply an act of EU law is not revoked even by the bringing of an action for annulment.⁹ It is all the more the case that the revelation of facts, even essential facts as in the present case, cannot be put forward as a circumstance which renders invalid, or even removes the obligation to apply, a formally binding act of EU law.

II.2. Possibility of authorities of a Member State suspending the transfer of data to the United States

- 10 However, the Republic of Poland notes that in the present case there is no need to question the lawfulness of Decision 2000/520 or the obligation to apply it. The decision laid down a mechanism enabling remedial action to be taken where there are irregularities in the organisation to which personal data are transferred.
- 11 Decision 2000/520 authorises the competent authorities of the Member States to suspend the flow of data in certain circumstances. As recital 8 of the preamble to that decision states, '[i]n the interests of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify in this Decision the exceptional circumstances in which the suspension of specific data flows should be justified, notwithstanding the finding of adequate protection'. Those exceptional circumstances were detailed in Article 3(1)(b) of the decision. Under that provision, the competent authorities may suspend data flows to an organisation that has self-certified its adherence to the principles implemented in accordance with the frequently asked questions in order to protect individuals with regard to the processing of their personal data in cases where:
 - (1) there is a substantial likelihood that the principles are being violated;
 - (2) there is a reasonable basis for believing that the enforcement mechanism is not taking or will not take adequate and timely steps to settle the case at issue; and
 - (3) the continuing transfer would create an imminent risk of grave harm to data subjects.
- 12 Therefore, in the cases referred to above the competent authorities of the Member States may suspend the flow of data to certain organisations, even though in principle the decision allows data to be transferred to them. It is clear that the authorisation of the competent authorities to suspend the flow of data in the above

⁸ Judgment in *CIVAD*, C-533/10, EU:C:2012:347, paragraph 39 and the case-law cited.

⁹ Judgment in *Commission v France*, C-261/99, EU:C:2001:179, paragraph 18.

circumstances also authorises them to examine independently whether such circumstances obtain.

- 13 This means that, in the event of doubt, the national authority for the protection of personal data — acting pursuant to Decision 2000/520 — may examine the facts and, on the basis of the findings made, if the circumstances referred to in Article 3(1)(b) of that decision obtain, suspend the flow of data from the Member State concerned to organisations in a third country, in this case the United States, where the organisations concerned are recognised as ensuring an adequate level of data protection.

II.3. Transfer of personal data to the United States in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union

- 14 In its request for a preliminary ruling, the national court casts doubt on the compatibility of Decision 2000/520 with the Charter of Fundamental Rights of the European Union, referring in that context to Articles 7 and 8 thereof. Those provisions lay down the right to the protection of personal data which is derived historically from the right to respect for private life.¹⁰
- 15 The referring court states that personal data are transferred to the United States where there is potentially mass and undifferentiated accessing of such data. In that context it should be noted that the ability of competent national authorities to access personal data is regarded, by both the European Court of Human Rights and the Court of Justice of the European Union, as further interference with fundamental rights.¹¹ However, such limitations are sometimes permissible because the right to protection of personal data is not absolute. As the Court of Justice has held, derogations and limitations in relation to the protection of personal data must nevertheless apply only in so far as is strictly necessary.¹² Article 52(1) of the Charter also states that subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. Such a limitation is also permitted by the Safe Harbour scheme, provided that the principle of necessity is observed. In

¹⁰ As Advocate General Jääskinen stated in his Opinion in *Spain and Google* (C-131/12, EU:C:2013:424, points 112 to 118 and the case-law cited), on the basis of the case-law of the European Court of Human Rights the protection of private life under the Charter covers all information relating to an individual ... and any act of communication relying on automatic means such as by means of social media concerning a natural person constitutes as such a putative interference of that fundamental right.

¹¹ Judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 35 and the case-law cited.

¹² Judgments in *Digital Rights Ireland and Others*, EU:C:2014:238, paragraph 52, and *IPI*, C-473/12, EU:C:2013:715, paragraph 39 and the case-law cited.

the light of the judgment in *Digital Rights Ireland and Others*, mass and undifferentiated accessing of data fails to fulfil the requirement relating to proportionality and is not justified by the objective of maintaining national security.

- 16 In assessing the limitations placed on fundamental rights by the activities of US federal agencies, a distinction must be drawn between the objective of those activities and the scope thereof. As regards the objective, the Court of Justice holds, in the wake of the judgments of the European Court of Human Rights, that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest.¹³ In its request the national court holds that that objective — the preservation of national security and the prevention of serious crime — is served by electronic surveillance and interception of personal data by the abovementioned federal agencies.
- 17 Although it does not question the compatibility of that objective with the law, the referring court highlights its uncertainty as regards the proportionality requirements which must be satisfied by any limitation of the right to protection of personal data. Therefore, it identifies a need to examine whether the processing of personal data transferred to organisations in the United States fulfils the proportionality requirements set out in the case-law of the Court of Justice, in particular in its judgment in *Digital Rights Ireland and Others*.
- 18 At the same time, the request for a preliminary ruling appears to show that the referring court did not consider the possibility of suspending the flow of data, a possibility provided for expressly in Decision 2000/520 in the cases specified in Article 3(1)(b) thereof. As a result, the referring court concludes that the assessment whether the transfer of personal data to the United States currently satisfies the requirements of EU law can be made only by examining the lawfulness of Decision 2000/520 in the light of the Charter.
- 19 In that context, the Republic of Poland points out that the competent national authorities cannot refuse to apply Decision 2000/520 on the ground that they consider it to be incompatible with the Charter. However, that decision does give national authorities a control tool which enables them to examine, for the purposes of a specific case, whether or not there is a risk of disproportionately limiting the fundamental rights laid down in Articles 7 and 8 of the Charter. That decision allows national authorities to suspend the transfer of data to organisations in the United States where, according to their findings, there is a risk of the right to data protection being infringed.¹⁴

¹³ Judgment in *Digital Rights Ireland and Others*, EU:C:2014:238, paragraph 42 and the case-law cited.

¹⁴ The existence of such a possibility was also highlighted recently by the Data Protection Working Party, which at the same time noted that the scope of that

- 20 Therefore, the general principle relating to the adequacy of the personal data protection provided by bodies certified under the Safe Harbour scheme is not absolute in the light of Article 3 of Decision 2000/520. The possibility of suspending the flow of data in the circumstances set out in that provision is an expression of the EU legislature's concern for a high level of personal data protection and it safeguards against the automatic transfer of data in all circumstances. Consequently, in the view of the Republic of Poland the doubts raised by the referring court as to the compatibility of Decision 2000/520 with EU personal data protection standards do not arise in so far as they stem from an incorrect assumption that the national authority for the protection of personal data is absolutely bound by the principle, arising from that decision, as to the adequacy of the data protection provided by bodies certified under the Safe Harbour scheme.
- 21 It should also be noted that Decision 2000/520 was adopted pursuant to Directive 95/46 which, as the Court of Justice has pointed out, seeks 'to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data'.¹⁵ The importance of fundamental rights in the context of the protection of personal data was emphasised in that directive, which states that where personal data are processed, the fundamental rights and freedoms of physical persons, notably the right to privacy, must be respected.¹⁶
- 22 Decision 2000/520 lays down the framework for the system of protection for personal data which, if applied correctly by US organisations, can allow an adequate level of protection for personal data held by those organisations in the United States. That decision also points out that the system established by it can operate properly only if the organisations participating in it adhere to the principles laid down therein.¹⁷ In addition to the principles and the frequently asked questions contained in the annexes to the decision, US organisations must also adhere to all the principles adopted by the US Department of Commerce as a result of Commission recommendations to the US Government, also issued as a consequence of reports in 2013. Only complete compatibility of the activities of the US organisations participating in Safe Harbour with the rules currently laid down, together with effective cooperation between the European Union and United States, can result in a guarantee of an adequate level of protection for personal data.
- 23 When examining the facts of a specific case pursuant to Article 3(1)(b) of Decision 2000/520, the national authority for the protection of personal data can

possibility should be clarified and specified (document ref.: Ares(2014)1139376 — 10/04/2014, p. 1).

¹⁵ See, for example, judgment in *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraphs 53 and 66.

¹⁶ Directive 95/46, recital 2.

¹⁷ Decision 2000/520, recital 5.

take measures to ascertain whether US organisations to which the defendant's personal data are transferred are in fact adhering to the principles laid down in the decision and by the US Department of Commerce. If, on the basis of the information obtained, that authority finds that there is a substantial likelihood that those principles are being violated, it can suspend the flow of data to the organisation concerned. When examining the facts of each case and taking any decision on suspending the flow of data, the national authority for the protection of personal data must have regard to Articles 7 and 8 of the Charter.

III. Proposed decision

- 24 In the light of the arguments set out above, the Republic of Poland proposes that the Court of Justice of the European Union answer the question referred by the national court as follows:

In the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding contained in Commission Decision 2000/520/EC of 26 July 2000 having regard to Article 7, Article 8 and Article 47 of the Charter of Fundamental Rights of the European Union, the provisions of Article 25(6) of Directive 95/46/EC notwithstanding. However, the office holder may, in any case provided for in Article 3(1)(b) of Decision 2000/520/EC, conduct his or her own investigation of the matter, inter alia in the light of factual developments since that decision was first published, and also, as a result of the procedure, suspend the flow of data to an organisation certified under the Safe Harbour scheme, in particular where there is reason to suspect that there is a substantial likelihood that the Safe Harbour principles are being violated.

Bogusław Majczyna

Agent of the Republic of Poland